UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,536	08/03/2001	John R. McGarvey	5577-236	6803

20792 7590 08/04/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,536	MCGARVEY ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 5/19/2005.

Response to Arguments

Applicant's arguments with respect to claims 1-32 have been considered but are moot in view of the new ground(s) of rejection.

DETAILED ACTION

All objections and rejections not set forth below have been withdrawn.

Claims 1-32 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 23-25, and 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brezak et al. (US Patent Application Publication 2003/0018913) hereinafter referred to as Brezak, and further in view of Ganesan (US Patent Number 5,535,276).

Regarding claim 1, Brezak disclosed a method for a middle tier server to impersonate a client to a plurality of servers, the method comprising: obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043 "service ticket"); providing the common nonce to the client (See Brezak Fig. 2 Paragraph 0043 Lines 3-6)); receiving the common nonce at the middle

tier server (See Brezak Paragraph 0043 Lines 6-9), and providing the common nonce as a signature for transactions for the client to the plurality of servers so as to authenticate the client to the plurality of servers (See Brezak Paragraph 0044 and Paragraph 0055 Lines 12-14).

However, Brezak failed to disclose the client signing the common nonce (service ticket).

Ganesan teaches that in a ticketing system, in order to protect against dictionary attacks, the ticket should be encrypted by the ticket granting system with the key shared between the server to be accessed and the ticket granting server (See Ganesan Col. 5 Lines 34-56), and the user should sign the ticket (TEMP-CERT) (See Ganesan Col. 15 Lines 45-60).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Ganesan in the ticketing system of Brezak by having the ticket encrypted with server/ticket granting system keys, and having the client sign the service ticket before sending the ticket to the Server A. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against dictionary attacks against the ticket.

Regarding claim 26, the combination of Brezak and Ganesan disclosed a system for a middle tier server to impersonate a client to a plurality of servers, the system comprising: means for obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043 "service ticket"); means for providing the common nonce to the client (See Brezak Fig. 2 Paragraph 0043 Lines 3-6)); means for receiving the common nonce singed by the client at the middle tier server (See Brezak Paragraph 0043 Lines 6-9 and Ganesan Col. 15 Lines 45-60), and means for providing the common nonce as a signature for transactions for the client to the plurality of

servers so as to authenticate the client to the plurality of servers (See Brezak Paragraph 0044 and Paragraph 0055 Lines 12-14).

Regarding claim 27, the combination of Brezak and Ganesan disclosed a computer program product (See Brezak Paragraph 0015) for a middle tier server to impersonate a client to a plurality of servers, comprising: a computer readable media having computer readable program code embodied therein, the computer readable program code comprising: computer readable program code that obtains a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers (See Brezak Fig. 2 and Paragraph 0043 "service ticket"); computer readable program code that provides the common nonce to the client (See Brezak Fig. 2 Paragraph 0043 Lines 3-6)); computer readable program code that receives the common nonce singed by the client at the middle tier server (See Brezak Paragraph 0043 Lines 6-9 and Ganesan Col. 15 Lines 45-60), and computer readable program code that provides the common nonce as a signature for transactions for the client to the plurality of servers so as to authenticate the client to the plurality of servers (See Brezak Paragraph 0044 and Paragraph 0055 Lines 12-14).

Regarding claim 28, the combination of Brezak and Ganesan disclosed a method of authenticating a client, comprising: receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers from an entity other than the client of the plurality of servers (See Brezak Paragraph 0048), the common nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and authenticating the client based on the received signed common nonce (See Brezak Paragraph 0048).

Regarding claim 31, the combination of Brezak and Ganesan disclosed a system for authenticating a client, comprising: means for receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers from an entity other than the client of the plurality of servers (See Brezak Paragraph 0048), the common nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and means for authenticating the client based on the received signed common nonce (See Brezak Paragraph 0048).

Regarding claim 32, the combination of Brezak and Ganesan disclosed a system for authenticating a client, comprising: means for receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers from an entity other than the client of the plurality of servers (See Brezak Paragraph 0048), the common nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and means for authenticating the client based on the received signed common nonce (See Brezak Paragraph 0048).

Regarding claim 33, the combination of Brezak and Ganesan disclosed a computer program product for authenticating a client, comprising: a computer readable media having computer readable program code embodied therein (See Brezak Paragraph 0015), the computer readable program code comprising: computer readable program code which receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers from an entity other than the client of the plurality of servers (See Brezak Paragraph 0048), the common nonce being signed by the client (See Ganesan Col. 15 Lines 45-60), and computer readable program code which authenticates the client based on the received signed common nonce (See Brezak Paragraph 0048).

Regarding claims 2 and 30, the combination of Brezak and Ganesan disclosed that the common nonce is generated based on information provided by each of the plurality of servers (See Ganesan Col. 5 Lines 34-56).

Regarding claim 23, the combination of Brezak and Ganesan disclosed that the step of obtaining a common nonce comprises the steps of: obtaining the common nonce from a party trusted by the middle-tier server and the plurality of servers, the common nonce being signed by the trusted party; and verifying the signature of the common nonce is the signature of the trusted party (See the rejection of claim 1 above, especially Ganesan Col. 5 Lines 34-56).

Regarding claim 24, the combination of Brezak and Ganesan disclosed that at least one of the plurality of servers carries out the steps of: receiving a client certificate, determining if the client certificate is trusted; and indicating that the client is not authenticated if the client certificate is not trusted (See Brezak Paragraph 0055).

Regarding claim 25, the combination of Brezak and Ganesan disclosed that at least one of the plurality of servers carries out the steps of: receiving the signed common nonce and a client certificate; determining if the signature of the signed common nonce corresponds to a signature of the client certificate; and indicating that the client is not authenticated if the signature of the signed common nonce does not correspond to the signature of the client certificate (See Ganesan Col. 16 Line 64 – Col. 17 Line 5 and Col. 17 Lines 56-61).

Regarding claim 29, the combination of Brezak and Ganesan disclosed that the common nonce is provided by a trusted third party (See Brezak Paragraph 43).

Claims 3, 5, 7-11, and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Brezak and Ganesan as applied to claim 2 above, and further in view of Ford (US Patent Number 6,829,356).

Regarding claim 3, Brezak and Ganesan disclosed generating the common nonce based on information obtained from each of the plurality of servers (See the rejection of claim 2 above), but failed to disclose obtaining pre-nonce contributions from the plurality of servers; combining the pre-nonce contributions to provide a single pre-nonce token; and providing the common nonce based on the pre-nonce token.

Ford teaches a system in which a client can authenticate to a plurality of servers by signing proof data generated from a plurality of nonces associated with a plurality of servers (See Ford Col. 15 Line 9 – Col. 16 Line 14) involving obtaining pre-nonce contributions from the plurality of servers (See Ford Col. 15 Lines 24-31); combining the pre-nonce contributions to provide a single pre-nonce token; and providing the common nonce based on the pre-nonce token (See Ford Col. 15 Lines 56-61).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Ford in the ticketing and authentication system of Brezak and Ganesan by providing the ticket granter with server nonces, combining the nonces, and placing the nonces in the ticket to be signed. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide strong secret data which could be verified in the ticket.

Regarding claim 5, the combination of Brezak, Ganesan, and Ford disclosed that the step of combining the pre- nonce contributions to provide a single pre-nonce token comprises concatenating the pre-nonce contributions (See Ford Col. 15 Lines 56-61).

Regarding claim 7, the combination of Brezak, Ganesan, and Ford disclosed that the step of obtaining pre-nonce contributions comprises the steps of: requesting a pre-nonce contribution from each of the plurality of servers (See Ford Col. 15 Paragraph 2); and receiving the pre-nonce contributions from the plurality of servers (See Ford Col. 15 Paragraph 2).

Regarding claim 8, the combination of Brezak, Ganesan, and Ford disclosed that requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of servers (See Ford Col. 15 Lines 1-22).

Regarding claim 9, the combination of Brezak, Ganesan, and Ford disclosed the step of encrypting the authenticated requests sent to the plurality of servers (See Ford Col. 15 Paragraph 1).

Regarding claim 10, the combination of Brezak, Ganesan, and Ford disclosed that the authenticated requests include at least one of an identification of a source of the request, a time stamp and a random number (See Brezak Paragraph 0051).

Regarding claim 11, the combination of Brezak, Ganesan, and Ford disclosed that the pre-nonce contributions include at least one of an identification of a server of the plurality of servers and a random number (See Ford Col. 15 Lines 24-38, and Line 56 Col. 16 Line 2).

Regarding claim 14, the combination of Brezak, Ganesan, and Ford disclosed the steps of: receiving a transaction identification from a trusted server of the plurality of servers; and

associating the transaction identification with the common nonce (See Ford Col. 15 Lines 22-31).

Regarding claim 15, the combination of Brezak, Ganesan, and Ford disclosed the step of tracking use of the common nonce based on the transaction identification (See Ford Col. 15 Line 22 - Col. 16 Line 2).

Claims 4, 6, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Brezak, Ganesan, and Ford as applied to claim 3 above, and further in view of Schneier (Applied Cryptography).

Regarding claim 4, the combination of Ford and Blakley disclosed providing a common nonce (See Ford Col. 15 Lines 56-61), but failed to disclose reducing the nonce challenges to provide the common nonce. However, Ford and Blakley did disclose digitally signing a message containing the nonce challenges (See Ford Col. 15 Lines 56-61).

Schneier teaches that when digitally signing a message, it is practical to hash the message and encrypt the hash, with a private key, as the signature, rather than encrypting the whole message (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions). Schneier also teaches that in such a system, to verify the signature, the verifier hashes the message, decrypts the signed hash with the signers public key, and verifies that the two hashes are the same (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the digital signatures of Brezak, Ganesan, and Ford by signing and verifying the hash of the nonce message instead of the whole nonce

message. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the speed of the signing method.

Regarding claim 6, the combination of Brezak, Ganesan, Ford, and Schneier disclosed that the step of reducing the pre-nonce token to provide the common nonce comprises the step of hashing the pre-nonce token utilizing a one-way hash function so as to provide the common nonce (See the rejection of claim 4 above).

Regarding claim 20, the combination of Brezak, Ganesan, Ford, and Schneier disclosed that at least one of the plurality of servers carries out the steps of: receiving the signed common nonce, the common nonce and the pre-nonce token; hashing the received pre-nonce token; comparing the hashed pre-nonce token to the common nonce; indicating that the client is not authenticated if the hashed pre-nonce token is different from the common nonce (See Ford Col. 15 Lines 56-65 and Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

Regarding claims 12-13, the combination of Brezak, Ganesan, and Ford disclosed the client checking the nonce challenge from the server for requisite strength, and aborting the authentication process if the nonce challenge did not meet the requisite strength (See Ford Col. 15 Lines 39-41), but failed to disclose that this check included checking the signature of the nonce challenge to verify that it was signed by the server.

Schneier teaches that digital signatures provide a means for verifying the sender of a message (See Schneier Page 37 Signing Documents with Public Key Cryptography).
It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the nonce challenge system of Ford and Blakley by having

the server sign the challenges and having the client verify the signature of the challenges before using the challenges. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against illicit alteration of the challenge nonce.

Claims 16-19, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Brezak, Ganesan, and Ford as applied to claim 3 above, and further in view of Menezes et al. (Handbook of Applied Cryptography).

The combination of Brezak, Ganesan, and Ford disclosed the server receiving the nonce challenges, and authenticating the client based on whether the nonce challenges included the nonce challenge of the server (See Ford Col. 15 Lines 56-65), but failed to disclose that the nonce challenges included random numbers. The combination further disclosed using a users public key to verify the signature of the nonce message by verifying that the signature corresponded to the signature of the clients private/public key pair (See Ford Col. 15 Lines 56-65), but failed to disclose that the verifying server got the public key from a public key certificate and also failed to disclose that the authentication would fail if the certificate was not trusted.

Menezes teaches that nonce challenges can be random numbers (See Menezes Page 398). Menezes further teaches that when using nonce challenges the challenger should apply a timeout period to the nonce and not authenticate the client if the response is received after the timeout period has expired (See Menezes Page 398 Section (i)). Menezes teaches further still that public key certificates are a means to store, distribute, and forward public keys without danger of undetectable manipulation. Menezes also teaches that when using a certificate for authentication, the certificate is received, the expiration date is checked, the certification authority validity is checked, the signature of the certificate is checked, and the certificate is

checked to see if it has been revoked, and if these checks pass then the public key is valid (See Menezes Pages 559-560).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the nonce challenge system of Brezak, Ganesan, and Ford by having the nonce challenges be random numbers and by applying and checking a timeout period to the nonce when authenticating a client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide uniqueness and timeliness assurances in the system in order to avoid replay and interleaving attacks. It further would have been obvious to employ the teachings of Menezes in the authentication system of Brezak, Ganesan and Ford by obtaining the public key from a public key certificate and verifying that the certificate is valid in order to use the public key to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against undetected manipulation of the public key.

Conclusion

Claims 1-32 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Brezak et al. (US Patent Application Publication 2002/0150253) disclosed a system in which a server authenticates a client and once authenticated the server presents authentication information to a plurality of servers.

Bartolomeos et al. (PCT Publication WO 99/56194) disclosed a system in which a server authenticates a client and then provides authentication of the client to a plurality of other servers.

Damour et al. (European Patent Application EP1168763) disclosed a system in which a server authenticates a client using nonce challenges and then delegates the authorization to other servers.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
7/26/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100